

Page 3 of 18
Application. No. 10/032,228
Amendment A

Amendments To The Claims

Claim 1 (currently amended): An apparatus comprising:

- a first encryption key storage unit configured to store a first encryption key;
- a second encryption key storage unit configured to contain a second encryption key;
- an encryption unit configured to encrypt a message containing ~~[[a]]~~ the first encryption key,
the message encrypted with the second encryption key;
- a radio configured to transmit the message over a wireless network and configured to receive
a subsequent message over the wireless network, the subsequent message encrypted with the first
encryption key.

Claim 2 (currently amended): The apparatus of claim 1, further comprising:

- a decryption unit configured to decrypt the subsequent ~~[[a reply]]~~ message received from the
radio, ~~the reply message encrypted with the first encryption key.~~

Claim 3 (currently amended): The apparatus of claim 2, further comprising:

- a protocol management unit configured to convey the subsequent ~~[[reply]]~~ message to a host
device.

Claim 4 (original): The apparatus of claim 3, further comprising:

- a selector configured to select between the encryption key storage units as input to the
encryption unit and decryption unit.

Claim 5 (original): The apparatus of claim 4, further comprising:

- a device control unit configured to aid the selector in the selection between the encryption
key storage units.

Claim 6 (original): The apparatus of claim 5 wherein the second encryption key is symmetric.

Claim 7 (original): The apparatus of claim 6 wherein the first encryption key is symmetric.

432323_1

Page 4 of 18
Application No. 10/032,228
Amendment A

Claim 8 (currently amended): The apparatus of claim ~~[[7]]~~ 1 wherein the second encryption key is a peripheral device encryption key.

Claim 9 (original): The apparatus of claim 8 wherein the first encryption key is a host device encryption key.

Claim 10 (currently amended): The apparatus of claim 9 wherein the peripheral device encryption key is received ~~from human input to the~~ by a host device via input by a user.

Claim 11 (currently amended): The apparatus of claim 10, wherein the protocol management unit is configured to convey the subsequent ~~[[reply]]~~ message to the host device via the Universal Serial Bus protocol.

Claim 12 (currently amended): A method comprising:
receiving, at a module, a second encryption key;
transmitting, ~~from the module~~, a message containing a first encryption key over a wireless network, the message encrypted with the second encryption key; and
receiving, at a module, a subsequent message encrypted with the first encryption key.

Claim 13 (canceled)

Claim 14 (currently amended): The method of claim ~~[[13]]~~ 12 further comprising:
decrypting the subsequent ~~[[reply]]~~ message with the first encryption key.

Claim 15 (original): The method of claim 14 wherein the second encryption key is symmetric.

Claim 16 (original): The method of claim 15 wherein the first encryption key is symmetric.

432323_1

Page 5 of 18
Application No. 10/032,228
Amendment A

Claim 17 (currently amended): The method of claim [[16]] 12 wherein the second encryption key is a peripheral device encryption key.

Claim 18 (original): The method of claim 17 wherein the first encryption key is a host device encryption key.

Claim 19 (currently amended): The method of claim 18 wherein the peripheral device encryption key is received ~~from human input~~ by a host device via input by a user.

Claim 20 (original): The method of claim 18 wherein the host device encryption key is stored within an encryption key storage unit.

Claim 21 (currently amended): The method of claim [[18]] 20 wherein the encryption key storage unit that stores the host device encryption key is a read only memory.

Claim 22 (currently amended): The method of claim 21 further comprising:
sending the decoded subsequent [[reply]] message to a host using a Universal Serial Bus interface.

Claim 23 (currently amended): A computer-readable medium encoded with data and instructions, the data and instructions causing an apparatus executing the instructions to:

receive, at a module, a second encryption key;
transmit, from the module, a message containing a first encryption key over a wireless network, the message encrypted with the second encryption key; and
receive, at the module, a subsequent message encrypted with the first encryption key.

Claim 24 (canceled)

Claim 25 (currently amended): The computer-readable medium of claim [[24]] 23, the instructions

432323_1

Page 6 of 18
Application No. 10/032,228
Amendment A

further causing an apparatus executing the instructions to:

decode the subsequent [[reply]] message with the first encryption key.

Claim 26 (original): The computer-readable medium of claim 25 wherein the second encryption key is symmetric.

Claim 27 (original): The computer-readable medium of claim 26 wherein the first encryption key is symmetric.

Claim 28 (currently amended): The computer-readable medium of claim [[27]] 23 wherein the second encryption key is a peripheral device encryption key.

Claim 29 (original): The computer-readable medium of claim 28 wherein the first encryption key is a host device encryption key.

Claim 30 (currently amended): The computer-readable medium of claim 29 wherein the peripheral device encryption key is received ~~from human input~~ by a host device via input by a user.

Claim 31 (original): The computer-readable medium of claim 29 wherein the host device encryption key is stored within an encryption key storage unit.

Claim 32 (original): The computer-readable medium of claim 29 wherein the encryption key storage unit that stores the host device encryption key is a read only memory.

Claim 33 (currently amended): The computer-readable medium of claim 32, the instructions further causing an apparatus executing the instructions to:

sending the decoded subsequent [[reply]] message to a host using a Universal Serial Bus interface.

432323_1

Page 7 of 18
Application No. 10/032,228
Amendment A

Claim 34 (currently amended): An apparatus comprising:

means for receiving, at a module, a second encryption key;
means for transmitting, from the module, a message containing a first encryption key over a wireless network, the message encrypted with the second encryption key; and
means for receiving, at the module, a subsequent message encrypted with the first encryption key.

Claim 35 (canceled)

Claim 36 (currently amended): The apparatus of claim ~~[[35]]~~ 34 further comprising:

means for decoding the subsequent ~~[[reply]]~~ message with the first encryption key.

Claim 37 (original): The apparatus of claim 36 wherein the second encryption key is symmetric.

Claim 38 (original): The apparatus of claim 37 wherein the first encryption key is symmetric.

Claim 39 (currently amended): The apparatus of claim ~~[[38]]~~ 34 wherein the second encryption key is a peripheral device encryption key.

Claim 40 (currently amended): The apparatus of claim ~~[[17]]~~ 39 wherein the first encryption key is a host device encryption key.

Claim 41 (currently amended): The apparatus of claim 40 wherein the peripheral device encryption key is received ~~from human input~~ by a host device via input by a user.

Claim 42 (original): The apparatus of claim 41 further comprising: means for storing the host device encryption key.

Claim 43 (original): The apparatus of claim 42 further comprising:

432323_1

Page 8 of 18
Application No. 10/032,228
Amendment A

means for storing the peripheral device encryption key.

Claim 44 (original): The apparatus of claim 43 further comprising:
means for decrypting received messages.

Claim 45 (original): The apparatus of claim 44 further comprising:
means for encrypting messages to be transmitted.

Claim 46 (currently amended): The apparatus of claim 45 further comprising:
means for sending the decoded subsequent [[reply]] message to a host using a Universal Serial Bus interface.

Claim 47 (currently amended): An apparatus comprising:
a first encryption key storage unit configured to contain a first encryption key;
a radio configured to receive a message over a wireless network from a host and to transmit a subsequent message over the wireless network, the received message encoded with the first encryption key and containing a second encryption key, the subsequent message encrypted with the second encryption key;
a decryption unit configured to ~~unencrypt~~ decrypt the received message with the first encryption key;
at least one temporary key storage unit configured to store the second encryption key.

Claim 48 (currently amended): The apparatus of claim 47, further comprising:
an encryption unit configured to encrypt the subsequent [[a reply]] message with the second encryption key.

Claim 49 (original): The apparatus of claim 48, wherein the radio is further configured to receive data messages over the wireless network from the host, the data message encoded with the second encryption key.

432323_1

Page 9 of 18
Application No. 10/032,228
Amendment A

Claim 50 (original): The apparatus of claim 49, further comprising:

a selector configured to select between the encryption key storage units as input to the encryption unit and decryption unit.

Claim 51 (original): The apparatus of claim 50, further comprising:

a device control unit configured to aid the selector in the selection between the encryption key storage units.

Claim 52 (original): The apparatus of claim 51, further comprising:

a protocol management unit configured to convey the data message to a peripheral device.

Claim 53 (original): The apparatus of claim 52, wherein the protocol management unit is configured to convey the data message to a peripheral device via the Universal Serial Bus protocol.

Claim 54 (original): The apparatus of claim 53 wherein the first encryption key is symmetric.

Claim 55 (original): The apparatus of claim 54 wherein the second encryption key is symmetric.

Claim 56 (currently amended): The apparatus of claim ~~[[54]]~~ 47 wherein the first encryption key is a peripheral device encryption key.

Claim 57 (original): The apparatus of claim 56 wherein the second encryption key is a host device encryption key.

Claim 58 (currently amended): A method comprising:

receiving a message over a wireless network from a host, the message encoded with a first encryption key and containing a second encryption key;

decrypting the received message using the first encryption key, extracting the second

432323_1

Page 10 of 18
Application No. 10/032,228
Amendment A

encryption key;

encrypting messages with the second encryption key; and
sending the encrypted messages to the host.

Claim 59 (original): The method of claim 58 further comprising:
storing the second encryption key in an encryption key storage unit.

Claim 60 (canceled)

Claim 61 (currently amended): The method of claim [[60]] 59 wherein the first encryption key is symmetric.

Claim 62 (original): The method of claim 61 wherein the second encryption key is symmetric.

Claim 63 (currently amended): The method of claim [[62]] 58 wherein the first encryption key is a peripheral device encryption key.

Claim 64 (original): The method of claim 63 wherein the second encryption key is a host device encryption key.

Claim 65 (original): The method of claim 64 wherein the encryption key storage unit is a register.

Claim 66 (original): The method of claim 65 wherein the encrypted messages sent to the host are received through a Universal Serial Bus interface.

Claim 67 (currently amended): A computer-readable medium encoded with data and instructions, the data and instructions causing an apparatus executing the instructions to:

receive a message over a wireless network from a host, the message encoded with a first encryption key and containing a second encryption key;

432323_1

Page 11 of 18
Application No. 10/032,228
Amendment A

decrypt the received message using the first encryption key, extracting the second encryption key;

encrypt messages with the second encryption key; and
send the encrypted messages to the host.

Claim 68 (original): The computer-readable medium of claim 67, the instructions further causing an apparatus executing the instructions to:

store the second encryption key in an encryption key storage unit.

Claim 69 (canceled)

Claim 70 (currently amended): The computer-readable medium of claim [[69]] 68 wherein the first encryption key is symmetric.

Claim 71 (original): The computer-readable medium of claim 70 wherein the second encryption key is symmetric.

Claim 72 (currently amended): The computer-readable medium of claim [[71]] 67 wherein the first encryption key is a peripheral device encryption key.

Claim 73 (original): The computer-readable medium of claim 72 wherein the second encryption key is a host device encryption key.

Claim 74 (original): The computer-readable medium of claim 73 wherein the encryption key storage unit is a register.

Claim 75 (currently amended): The computer-readable medium of claim [[76]] 73 wherein the encrypted messages sent to the host were received through a Universal Serial Bus interface.

432323_1

Page 12 of 18
Application No. 10/032,228
Amendment A

Claim 76 (currently amended): An apparatus comprising:

means for receiving a message over a wireless network from a host, the message encoded with a first encryption key and containing a second encryption key;

means for decrypting the received message using the first encryption key, extracting the second encryption key;

means for encrypting messages with the second encryption key; and

means for sending the encrypted messages to the host.

Claim 77 (original): The apparatus of claim 76 further comprising:

means for storing the first encryption key.

Claim 78 (original): The apparatus of claim 77 further comprising:

means for storing the second encryption key.

Claim 79 (canceled)

Claim 80 (currently amended): The apparatus of claim ~~[[79]]~~ 78 wherein the first encryption key is symmetric.

Claim 81 (original): The apparatus of claim 80 wherein the second encryption key is symmetric.

Claim 82 (currently amended): The apparatus of claim ~~[[81]]~~ 76 wherein the first encryption key is a peripheral device encryption key.

Claim 83 (original): The apparatus of claim 82 wherein the second encryption key is a host device encryption key.

Claim 84 (original): The apparatus of claim 83 wherein the means for storing the second encryption key is a register.

432323_1

Page 13 of 18
Application No. 10/032,228
Amendment A

Claim 85 (original): The apparatus of claim 84 wherein the encrypted messages sent to the host were received through a Universal Serial Bus interface.

Claim 86 (new): The apparatus of claim 1 wherein the first encryption key is specific to a host device coupled to the radio.

Claim 87 (new): The method of claim 12 wherein the first encryption key is specific to a host device coupled to the module.

Claim 88 (new): The computer-readable medium of claim 23 wherein the first encryption key is specific to a host device coupled to the module.

Claim 89 (new): The apparatus of claim 34 wherein the first encryption key is specific to a host device coupled to the module.

Claim 90 (new): The apparatus of claim 47 wherein the second encryption key is specific to the host.

Claim 91 (new): The method of claim 58 wherein the second encryption key is specific to the host.

Claim 92 (new): The computer-readable medium of claim 67 wherein the second encryption key is specific to the host.

Claim 93 (new): The apparatus of claim 76 wherein the second encryption key is specific to the host.

432323_1